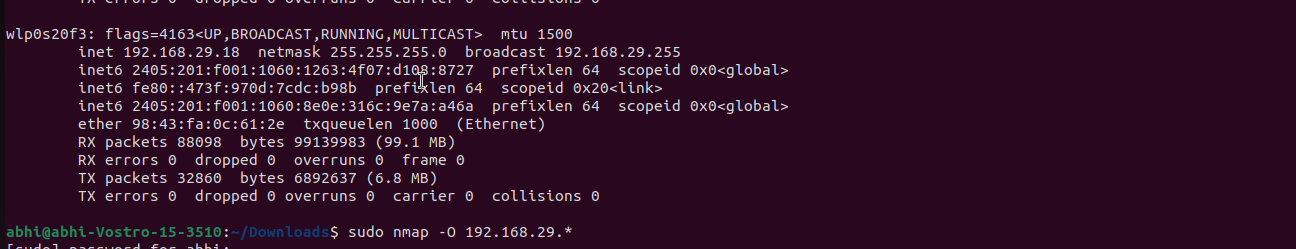
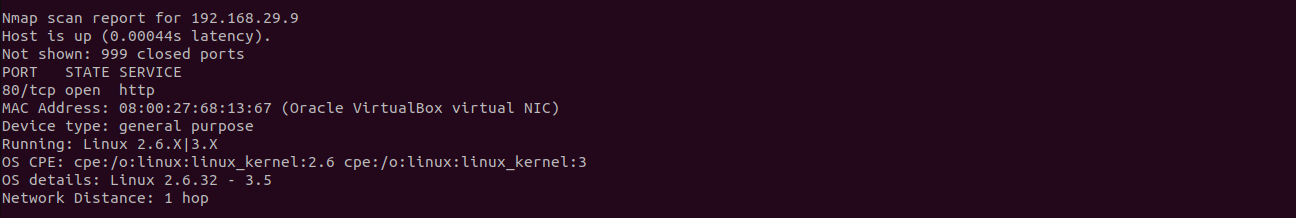
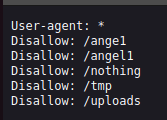
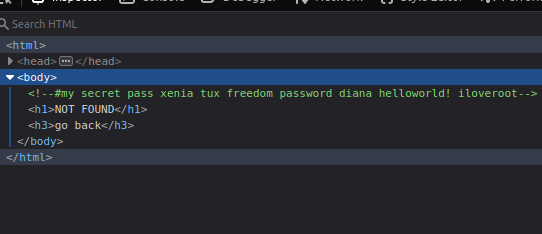
My first obstacle was figuring out how to connect to the server. But a little google showed that using ifconfig and then nmapping the ip  


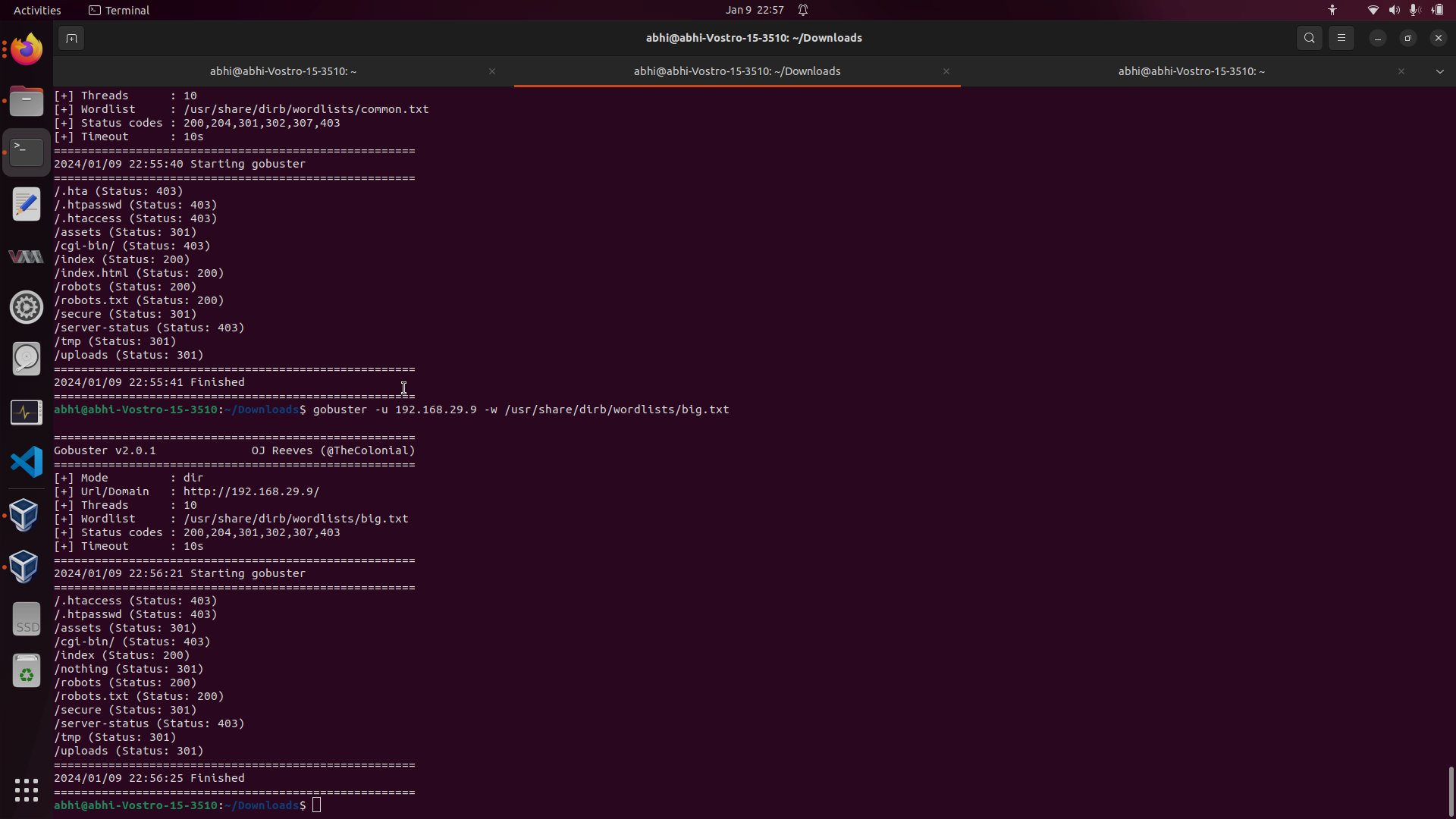
Opening the website, it was just an article and i couldnt find more. So i looked at the robots.txt.



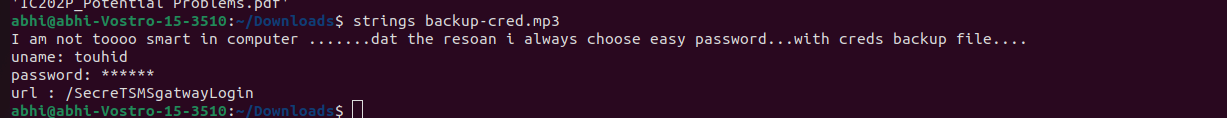
The only folder that yielded results was /nothing



But this really didnt help me, so i decided to use “gobuster”(a tool that bruteforces all existing directories). I wasn’t using my kali vm so i had to install “dirb” too for the wordlist.



The folder secure had a mp3 file which I promptly downloaded. But it seemed to be corrupted as my mp3 player could not run it. Running strings on it i got



http://<ip>/SecreTSMSgatwayLogin was a service called playSMS. Googling it gave me an exploit to run shell commands using PHP injection. This is the exploit I decided on using as it was streamlined for use and only involved typing the command.

But the user was “www-data” so i couldnt do much. Using the unspeakable power of google i learned of the forbidden technique “sudo -l”(i tried a lot of other commands too involving the sudoers file and so on. But this is what worked). It appeared i could use perl as sudo without a password. After that it was simple enough to retrieve the flag.